DST

Delta
Security
Technologies

ONR Projects to Provide Additional Cyber Security to NMCI

June 18, 2003

Corporate Profile

- Woman-owned small disadvantaged business
  - Corporate DoD facility clearance at the Secret level

- Three operating divisions
  - Security Services
  - Security Systems Engineering
  - Security Research and Development

- Three corporate facilities
  - Bay St. Louis, MS
    - HQ and R&D Facility at NASA Stennis Space Center
  - Alexandria, Virginia
  - Lexington Park, Maryland

Current ONR Security Projects for NMCI

1. NMCI Sentinel Project - Evaluate the production Sentinel‘s unique NMCI contributions through an integration project at an NMCI Facility.
2. DDLS Project - Develop a generic prototype of Dynamic Data Labeling System (DDLS) that sets remote access control policy from Smart Card.
3. Sentinel EFW Project - Develop Embedded Firewall (EFW) interoperability with Sentinel using Smart Cards to eliminate dependency on EFW Policy Server.

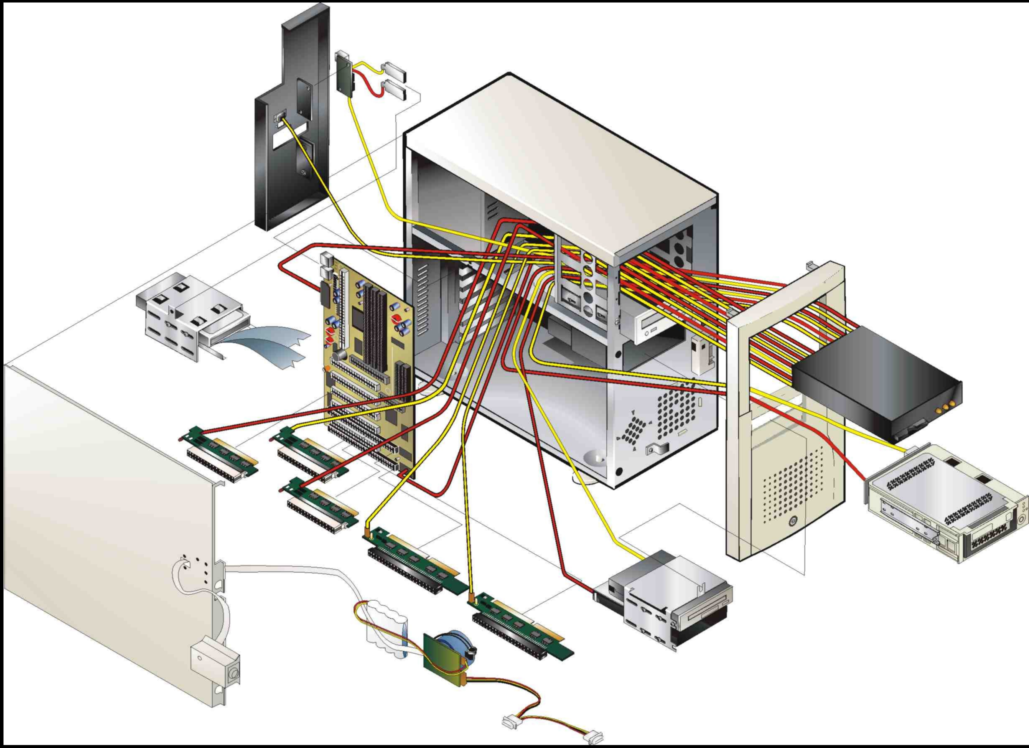
Sentinel-NMCI Project - Background

- Most organizations' valuable information and critical functions are vulnerable to exploitation by "INSIDERs" and "HACKERS"
- Users need 2 or 3 computers to separate multiple security levels of data; …still **CAN'T PROTECT data/functions from Insider attacks**

- **Sentinel Cyber Security System gives the organization total control over access** to its valuable information and critical operations:
  - Access is tailored to each User's security clearance and need-to-know/operate, implemented by User's Smart Card and **programmed by the organization**
  - Security controls are **independent of OS** and applications, tamper proof, and unobtrusive
- Can protect multiple security levels of data in **One Computer Console**

Sentinel-NMCI Project - Functional Description

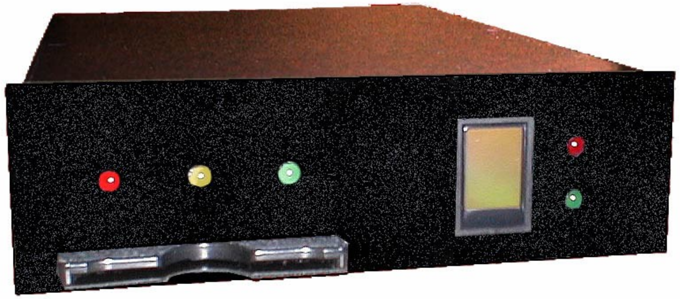
- Security Module provides hardware-based access control to components:
  - Network Interface Cards (NICs)
    - Standard NICs
    - Embedded Firewall (EFW) NICs
  - Modems (optional)
  - I/O ports (optional)
  - Hard Drives
    - Internal Hard Drive (s)
    - Removable Hard Drive (s)
  - Floppy Disk and/or ZIP Drives
  - CDROM or CD R/W Drive



Sentinel-NMCI Project -
Module Description

Secure Module includes:

- Micro-controller
  - Controls access to computer components IAW Users' security profile on Smart Card
  - Stores encrypted Program/Data
  - Tamper-resistant: memory erase; dummy-instruction features
- Smart Card Reader
- LEDs
  - Indicate interlocks satisfied and operating system can "boot-up"



Security Module

- Biometrics provide positive Identification of User to Security Module
  - Independent of computer's operating system and other authentication means

Sentinel-NMCI Project - Sentinel Status

- Awarded EAL4 rating by NIAP/NSA against 29 functions of Common Criteria; placed on Validated Products List, 28 August 2002
  - http://niap.nist.gov/cc-scheme/ValidatedProducts.html
  - Sentinel is the only computer security product to be successfully evaluated against a security target/profile that represents “Insider” threat.
- Awarded 3 U.S. Patents; 1 more pending
- Operational Evaluation completed in DARPA’s LAB
- Successfully evaluated in Department of State LAB
- Successfully evaluated by US Space Command
- Only security system evaluated against Insider Threat scenario
- Only cyber security system evaluated at EAL4 in categories: PC Access Control; Sensitive Data Protection
- NSA evaluation partially funded by PEO/IT because of its capability to significantly enhance NMCI enterprise security

Sentinel-NMCI Project -
Unique Contributions to NMCI

- Sentinel can provide EAL4 I&A of user to NMCI Terminal as a strong supplement for I&A of user to NMCI Server.
- Sentinel can provide strong EAL 4 I&A and Access Control necessary to protect current NMCI against Insider Attacks.
- Sentinel can meet object reuse requirement of NAVSO Pub 5239-15 by eliminating existing covert channels between classified users.
- Sentinel hardware-based Access Control can provide Mandatory Access Control between data on user’s removable hard drive (RHDD) and user thus preventing access to data by unauthorized users.
- Sentinel Hardware-Based Access Control can provide control of user access to classified data on RHDD and SIPRNET.
- Sentinel, with EAL4 rating, can support users’ need to access and process classified data at desktop within any PC.

Sentinel-NMCI Project - Potential Contributions to NMCI (Cont.)

- Sentinel can eliminate vulnerability due to writing classified data to a PC’s portable media (Floppy Disk, CD, DVD, Zip).
- Sentinel can use any ISO 7816 compliant Smart Card including CAC.
- Sentinel can provide time-of-day access control restrictions.
- Sentinel Smart Card administration can be done remotely using same process as is currently used to administer Smart Cards.
- Sentinel versatility allows Sentinel to be set up for any facility and for any workstation configuration including Thin Client.
- Sentinel provides both strong security and significant cost savings based on reductions in the number of computers required, support required, and technology refresh costs.

Establish Pilot Program for NMCI Integration

Implement research and development necessary to integrate Sentinel's <u>unique</u> capabilities into NMCI

- Provide Pilot Program at a designated Navy facility consisting of about ten (10) seats to refine Sentinel design and integrate & evaluate the more compact & less expensive Sentinel and its contributions to NMCI
  - NAVO recommended as Test Bed Facility due to proximity to DST's R&D Facility at Stennis Space Center, MS and status as an NMCI facility with unclassified and classified seats with SIPRNet and NIPRNet drops
- Pilot Program will:
  - Formally define and evaluate the NMCI/Sentinel architecture
  - Perform integration and evaluation of the Sentinel in the NMCI architecture

Sentinel Refinement Objectives

- **Reduce cost of production and purchase price to $300 per unit range**
- **Increase production efficiency and speed of delivery**
- **Improve supportability and reduce support costs**
- **Integrate and decrease number of components and size/cost of PCB’s using PLA Technology**
- **Change the hardware and form factor to implement Sentinel while using unchanged circuits and firmware preventing need for re-evaluation and maintaining EAL-4**
- **Produce a lower cost two level Sentinel based on same design by replacing the LCD Module with PIN/password acceptance LED indicators**
- **Eliminate the NVM Control Interface for applications where it is not required**

Sentinel-EFW Project - Background

- Current Embedded Firewall (EFW) is a NIC-based firewall that enforces a centrally-managed Security Policy

- EFWs protect networks from Insider Attacks … a capability NOT provided by perimeter firewalls
- Security Policy is currently managed and implemented by Policy Server
- DST is developing a capability to load User's Security Policy into EFW NIC from Sentinel Smart Card
  - Eliminates need for Policy Server
  - Enhances EFW security

Sentinel-EFW Project -
Develop EFW-Sentinel Interoperability

Implement development necessary to make EFWs interoperable with Sentinel using Smart Cards

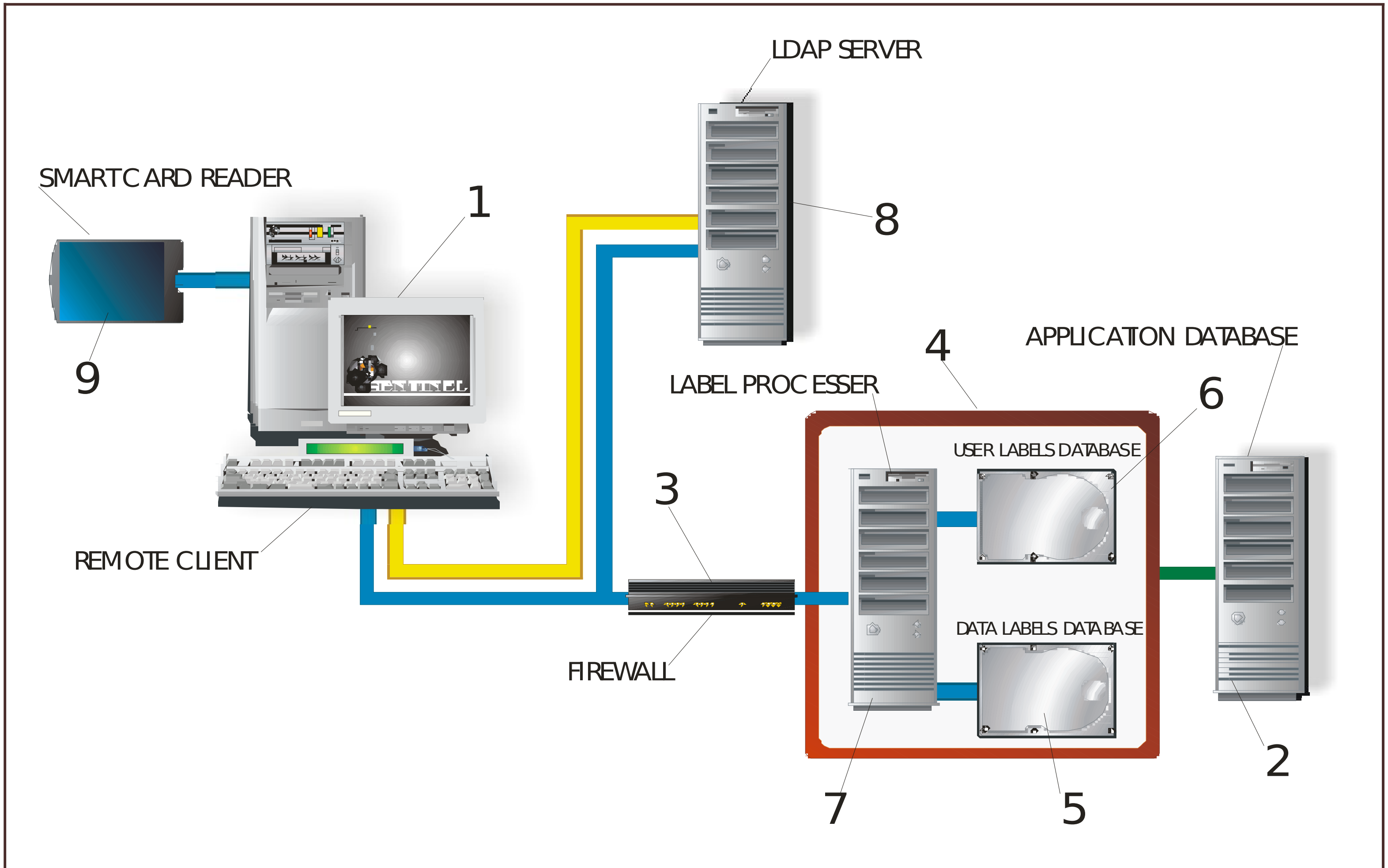
- DST, with assistance from 3COM, will develop and demonstrate the capability to load User's EFW Security Policy into EFW NIC from Sentinel User's Smart Card
  - DST's role in this Project will be to develop software/hardware interface for loading user's EFW security policy from Smart Card to EFW NIC
  - 3COM's role in this Project will be to develop the means, through software/firmware, to accept a User's Security Policy from the Sentinel's Smart Card

DDLS Project - Background

Unique capability to label categories / levels of data for WAN / Internet environment without disturbing the database

- Data Labeling MLS Enhancement (Data Labeler) provides data security through defined **security labels that provide Mandatory Access Control** (MAC) on digitized data.
  - **MAC (defined by DoD 5200.28-STD) is necessary to support the multi-level security** (MLS)/multi-category security (MCS) requirements of various security systems.
  - DDLS is capable of providing MAC for IPSec-based Virtual Private Networks (VPNs).
- Data Labeler developed for JEDMICS DoD system – successful prototype worked with hardware-based VPN solution.
- Data Labels are IAW National Standards and implemented external to the Database
  - Label format defined by the National Institute of Standards and Technology (NIST) in Federal Information Processing Standards Publication (FIPS PUB) 188, *“Standard Security Label for Information Transfer”*
- Data Labeler segregates data for access control into multiple data classification/sensitivity levels based on security attributes
  - Labels can be static or dynamically generated from data security attributes;
  - Labeling capability allows **256 different security levels and 65,535 categories of data** to be segregated in **any** common data base.
- Data labeler has 2 U.S. Patents Pending

DDLS Project - DDLS Architecture



Note: Numbers correlate to diagram in “White Paper” distributed separately

DDLS Project – Develop Generic Prototype DDLS

Implement research and development necessary to develop a Generic DDLS that will work within NMCI

- This Project will transform a specific application of DDLS, such as the one certified in the JEDMICS Program, into a generic data labeler that will work with any data base and IPSec-based VPN
  - This capability can be used to integrate existing legacy data bases into NMCI environment
  - Control access to E-Mail accounts and data as will be demonstrated for NMCI application
  - This Project will be conducted by DST at the Stennis R&D facility, the same facility that supported the development of the JEDMICS DDLS

Security Contributions to NMCI

- The NMCI contributions have been divided into three (3) different categories:

1. NMCI Capabilities Enhancement (New CLIN)
2. Contributions to existing CLIN 9
3. Value Additions to NMCI

1 - NMCI Capabilities Enhancement

- New capabilities could support establishing NEW CLIN to provide additional protection elements desired by “communities of interest” and significantly increase number of classified/CLIN 9-type seat requirements

  - Sentinel capability to authenticate user to computer and/or RHDD not available in present NMCI architecture

  - Sentinel capability to personalizes access to network not available in hardware in present NMCI architecture

1 a - Authenticates User to Computer/RHDD

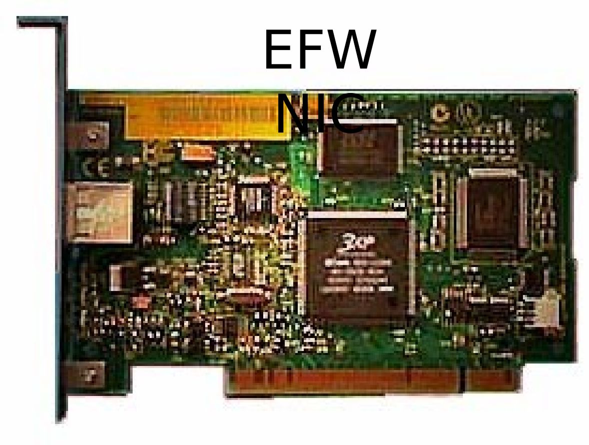
- Sentinel provides EAL4 rated I&A and Access Control to actual User Data in Removable Hard Drive (RHDD)
- Sentinel provides Fingerprint biometrics, with NO interface to the Operating System, to provide high assurance authentication
- Computer’s RHDD is electronically wedded to Sentinel’s Security Module and Smart Card

Security Module

- Access to Network, I/O ports, or modem are also controlled by user profile.
- Current computers in NMCI architecture have NO such protection

1 b – Personalizes Network Access

- Sentinel’s capability to provide hardware-based I&A to PC, when supplemented with EFW and DDLS, controls user’s access to network services, IP addresses, data categories, and external network access to PC
  - Sentinel hardware-based I&A ensures user’s security policy in Smart Card is linked to authenticated user & is secure from tampering when loaded in PC:
    - PIN is stored in user’s Smart Card
    - Password/Biometrics is stored in Sentinel
    - User Policy for PC/EFW/DDLS stored in Smart Card
  - EFW is NIC-based firewall with a user policy implemented for Packet Filtering
  - Sentinel I&A links PC access policy, EFW setup policy, and remote data access policy from Smart Card to authenticated user



2 – Sentinel Contributions to CLIN 9

2. Sentinel provides security contributions to CLIN 9 by providing increased protection at the classified terminal against existing threats:

   a. Protection against Insider Attacks by providing strong EAL4 hardware-based protection for computer terminal and network interface

   b. EAL4 Identification and Authentication (I&A) and Access control to RHDD and SIPRNET that supplements existing protection

   c. Elimination of covert channels between classified users to meet object reuse requirement of NAVSO Pub 5239-15

   d. Elimination of capability to write classified data to portable media

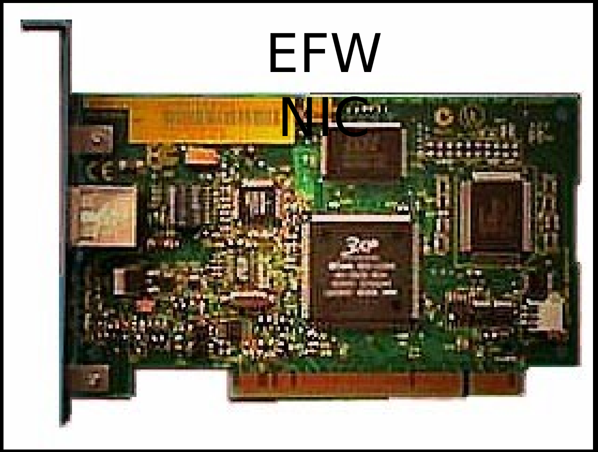
   e. Supplements security capabilities of Windows 2000 and applications without interference

   f. Provides a security capability above Secret Level

   g. Compatible with current CAC Smart Card

2 a - Reduce Vulnerability to Insider Threat

- Insider attacks responsible for more than 2/3 of all security intrusions
  - Insiders can be disgruntled employees, agents of foreign governments and/or terrorist organizations, criminals, and someone with a security clearance that is permitted access into the vaulted facility
- Many security solutions resemble “Maginot Line”… defenses that fortify the perimeter with firewalls/physical security that can be circumvented
- Sentinel, with EAL4 PC Access Control rating, restricts users to specified PC resources such as RHDDs and NICs - - dramatically reducing organization’s vulnerability to Inside



  - Sentinel can control access to network ports (turn ON/OFF):
    - Deny access to networks if ports are turned OFF;
    - Control access to networks if ports are turned ON through EFW NIC if user profile is on Sentinel’s Smart Card
  - Role separation, implemented by Sentinel, eliminates possibility of Administrator becoming an Insider Threat as a “Super User”

2 b – Provide Additional Controls Over User Access to Data and Network

- Sentinel provides Hardware Based Access Control to all computer ports including Network Interface Card (NIC) connected to SIPRNet
  - Sentinel allows each user to get access to classified data and the SIPRNET if they have the necessary classification and network access rights on their Smart Card
  - Individual users can be allowed access to classified data on RHDD without having access to SIPRNET
  - Provides flexibility in assigning a level of trust to individual users which can reduce security vulnerabilities and risks
- Sentinel can utilize EFW NICs and Smart Card to setup a hardware based firewall at the PC with a security policy for each user as part of Sentinel EAL4 I&A and Access Control Capability

2 c - Provide Object Reuse Protection

- Sentinel restricts Users from writing to Non-Volatile Memory (NVM) while in a restricted mode of operation
  - Sentinel EAL4 rating could not be awarded unless Sentinel demonstrated the capability to deny Users the ability to write to NVM in any host PC/workstation
  - NVMs can include the BIOS Chip, Video Card, and the Audio Card implemented in Flash Memory Technology

- If Classified Users are permitted to write to NVM, serious consequences follow:
  - Classified Users can pass on as many as 200 words per NVM of classified information to any Users (authorized or not) that gain access to the PC
  - This essentially establishes a Covert Channel
  - Violates NAVSO Pub 5239-15

2 d - Eliminate Ability to write Classified Data to Portable Media

- Sentinel EAL4 PC security policy eliminates vulnerability to unauthorized download of Classified data onto uncontrolled portable media devices (Floppys/CDRW/ZIP, etc.)
- Sentinel only allows Classified data to be stored on RHDDs that are access controlled to authorized data user to prevent access by unauthorized users
- Sentinel RHDDs cannot be accessed outside of a Sentinel-protected PC
- Sentinel RHDDs can only be accessed in a Sentinel-protected PC if the user has the proper I&A and security clearance
- Sentinel RHDDs can be setup to support RASP Media Encryption

2 e - Supplements Capabilities of Windows 2000

- Sentinel EAL4 security operates at the hardware level and is independent of the Operating System and software applications
- Sentinel EAL 4 security provides MAC and I&A to the hardware that supplements the DAC and I&A provided by Windows 2000 for data file and folder access
- Sentinel domain protection is at the RHDD, NIC, Modem, I/O port, NVM level as opposed to the data file/folder domain protection of Windows 2000
- Sentinel provides a role separation capability at the hardware level for Insider Attack protection that is not available in Windows 2000
- Sentinel provides a Failsafe and Physical Protection capability for the Classified seat that is not available in Windows 2000
- Sentinel RHDDs can support RASP Media Encryption under Windows 2000

2 f - Provides a Security Capability Above Secret

- Sentinel EAL4 Security Policy under the Common Criteria is independent of Classification Level
- Sentinel Security Policy will allow the Sentinel RHDDs to store data above the Secret Level with proper storage controls
- Sentinel-protected PC should be able to access and process data using standard Windows 2000 OS and applications at levels above Secret
- Hardware based Domain Separation and Residual Information Protection capability eliminates vulnerabilities in standard PCs that prevent operation above Secret Level
- RASP Media Encryption is not acceptable at levels above Secret

3 - Sentinel Value Additions to NMCI

- Sentinel value additions to all CLINs provide increased protection of, and control of access to, classified and/or restricted data:
  - Sentinel can be configured for Multilevel Access based on Periods Processing or the Single Level version can enhance the security of KVM-based domain separation
  - Sentinel provides the means to easily manage Legacy Applications in NMCI or Windows 2000-based environment
  - Sentinel can restrict access to terminals and networks based on the time of day
  - Versatility allows Sentinel to be set up for any facility and for any workstation configuration including Thin Client

Capability or Secure Simultaneous Access with KVM Switch

- Sentinel EAL4 rating with Domain Separation permits access to classified and unclassified data on separate Hard Drives in the same PC
  - Provides necessary separation for safe access, processing and storage of classified and sensitive data in ONE PC

- Sentinel installed in one processor for the protection of classified data, when coupled with another PC with a KVM switch, can provide secure access to classified and unclassified data simultaneously without rebooting

3 b – Legacy Application Management

- Sentinel with EAL4-rated Domain Separation provides means to quarantine Legacy Applications that fail to meet NMCI requirements
  - Sentinel can run the Legacy Application as a quarantined application inside Sentinel’s removable hard drive (RHDD)
  - Sentinel can control access to legacy network connection and any required I/O ports or modem connection
  - Eliminates the need to implement legacy application on a separate PC
  - When Legacy Application is eliminated or converted to NMCI application the transition does not require the elimination of the entire computer
  - Sentinel can securely support classified or unclassified legacy applications

3 C - Provide PC Access Control for Time-of-Day

- Security Administrator can reduce or eliminate each user’s access to the network, PC and/or RHDD based on time-of-day
  - This capability is implemented without interrupting ongoing sessions
  - Allows individual users to be setup for access to data and network during designated hours
  - Access to network can be setup differently than access to data on RHDD

- Sentinel time-of-day access control prevents after-hours intrusions into data and networks
  - Supplements physical security by allowing access to PCs/RHDDs and/or SIPRNET during working hours when required physical security is present

3 d - Sentinel Versatility Can Support all Classified CLINS in NMCI

- Sentinel’s versatility allows it to be set up for any user, facility, or workstation:
  - Users’ data and network access can be configured for security clearance and need-to-know requirements
  - Facility – Sentinel can be configured to enable access to only those NICs or I/O Ports that are required thus eliminating any potential vulnerabilities from interfaces that are not available
  - Workstation - Sentinel can be installed in any workstation configuration including:
    - Thin Client
    - 5 ¼ inch bay
    - 3 ½ inch bay
    - Internal to PC
    - External to PC

3e - Sentinel Provides Data Security w/o Encryption

- The Sentinel controls access to data based on Smart Card MAC, User I&A, and data access rights on Smart Card
- To gain access to data stored on a Sentinel RHDD the user must have:
  - Access to a Sentinel and a Smart Card that can be read by the Sentinel;
  - A Smart Card with a MAC that matches the MAC on the RHDD
  - Access rights on the Smart Card that match the access classification requirements of the RHDD
  - Knowledge of the correct PIN
  - Knowledge of the correct Password or possession of the required biometric
- The Sentinel RHDD creates a capability to securely transport user data with minimal data encryption
- Provides additional protection against unauthorized access to data even if data encryption is broken

Sentinel Cost-Benefits for NMCI

- Sentinel kit costs have fallen to almost 1/3 of what they were based on recent design refinements and advances in the electronics industry

- Costs of different models/configurations that benefit NMCI   vary with model/features selected:

  - Two-level model provides unique and additional security capabilities needed for NMCI classified and unclassified architectures
  - Less expensive than portrayed in current NMCI Schedule due to reduced hardware and support costs and the elimination of some Kit components
  - Eliminates need for an additional PC, KVM Switch and Keyboard Card Reader (KCR)
  - Versatility and hardware/software independence allows the Sentinel

Other Developments

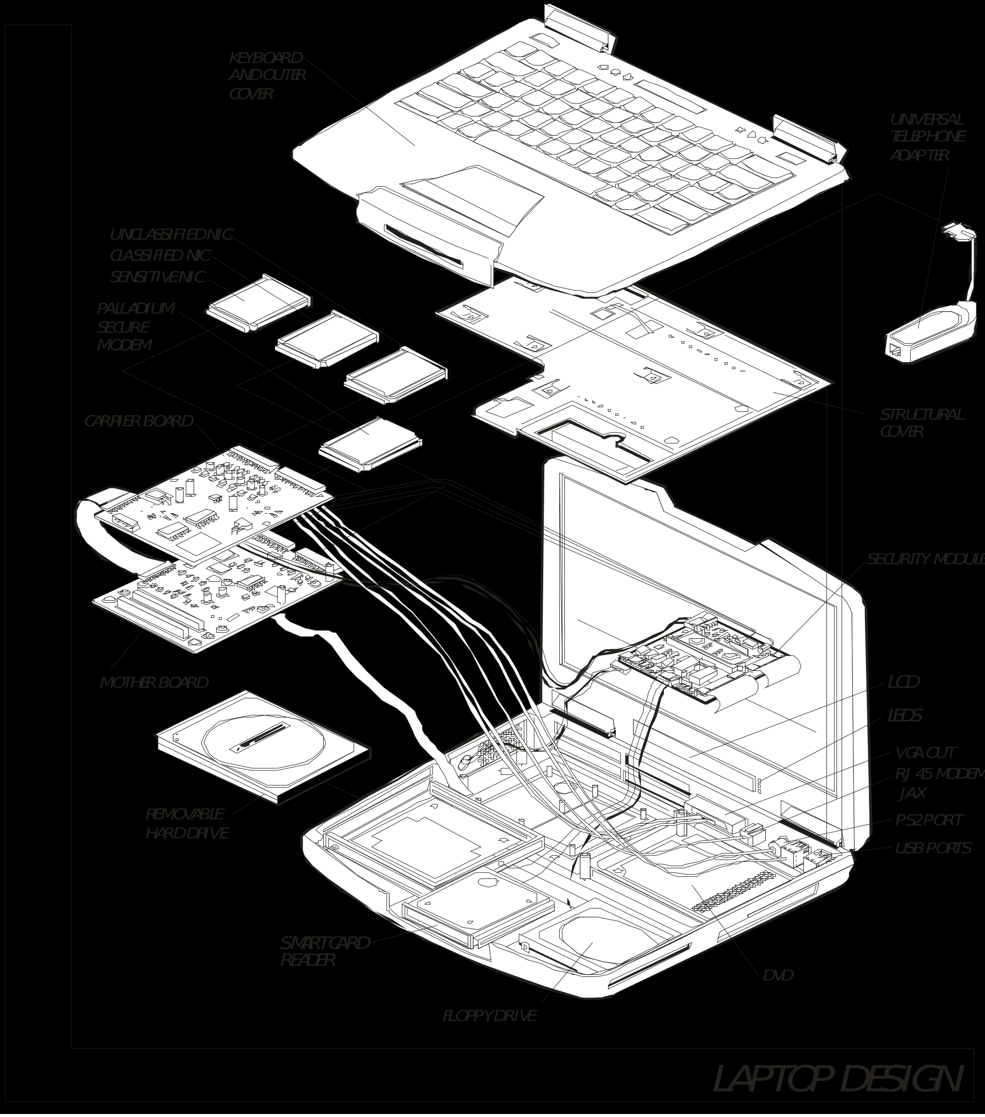
- A Laptop Version of the Sentinel is in development with the identical security capabilities, architecture, and user interface as the desktop system.

- DST is designing a hardware version of the client DDLS software that can be installed as a module within the Sentinel Kit and has the inherent protections against Insider Attacks provided by hardware based security products.

- DST is evaluating the requirements for implementing

Sentinel-Laptop Project

- Functionally and operationally identical to desktop model:
  - Will meet same security EAL4 evaluation requirements
  - Will use same Smart Card
  - Will support media encryption
- Implemented as a complete computer and not a kit with:
  - Pentium III/IV processor
  - Removable Hard Drives
  - 2 USB Ports, 3 NICs, and an internal CD-ROM/DVD
  - Weigh < 6 lbs
- Security Module provides hardware-based access control to components:
  - NICs) including Embedded Firewall (EFW) NICs in PCMCIA format
  - Modems (optional)
  - I/O ports
  - Removable Hard Drives
  - Floppy Disk
  - CDROM



DST

Delta
Security
Technologies

Cyber-Security for a Non-Secure World

For additional information contact:
Robert Clime
Director, Business Development
703-751-9515

Rclime@delta-sec.com
www.delta-sec.com